IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MONSANTO COMPANY,	)	
	)	
and	)	
	)	
THE CLIMATE CORPORATION,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	Case No. 4:16-cv-876
	)	
JIUNN-REN CHEN,	)	
	)	
and	)	
	)	
JOHN AND JANE DOES 1 THROUGH 10 AND OTHER JOHN DOE CORPORATIONS 1 THROUGH 10	)	
	)	
Defendants.	)	

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER

Plaintiffs, Monsanto Company and The Climate Corporation ("Plaintiffs" or "the Company"), file this Memorandum in Support of Their Motion for a Temporary Restraining Order against Defendant, Jiunn-Ren Chen ("Defendant" of "Mr. Chen"). Plaintiffs are entitled to a temporary restraining order preserving the status quo and preventing Defendant Jiunn-Ren Chen from causing further irreparable harm to Plaintiffs. Entrusted with access to Plaintiffs' confidential trade secrets and proprietary information, Defendant uploaded fifty-two files containing Plaintiffs' proprietary trade secret information from Plaintiffs' secure environment and sent them to an undisclosed location. Plaintiffs have alleged facts sufficient to support numerous claims against Defendant, most notably violations of the Defend Trade Secrets Act of

2016, recently enacted to protect innovative American companies such as Monsanto in instances just such as this.

FACTUAL BACKGROUND

Jiunn-Ren Chen was employed as a data science analyst by Monsanto Company, and also performed work for The Climate Corporation, a wholly-owned subsidiary of Monsanto Company. *See* attached Declarations of Scott B. Baucum and Brent A. McCarty. The Climate Corporation helps the world's farmers sustainably increase their productivity with digital tools. *Id.*The Climate Corporation uses proprietary algorithms and predictive analytics to enhance technological tools sold to farmers. *Id.* As such, confidential trade secrets are of vital importance and substantial value to Plaintiffs' current and future business interests. *Id.*

In his capacity as a data science analyst, Mr. Chen wrote code and/or algorithms that were of vital importance to Plaintiffs. *Id.* As part of his work for Plaintiffs in performing these duties, Mr. Chen helped create and thus had access to Plaintiffs' confidential trade secrets and proprietary information. *Id.* Mr. Chen had access to this information through both a PC computer issued to him by Monsanto and a Macintosh computer issued to him by The Climate Corporation. *Id.* Mr. Chen, as with other Monsanto employees, was assigned unique login credentials that allowed him to enter a secure electronic environment where he created, accessed, and collaborated in the production of critical proprietary information. *Id.* Ordinarily, within this secure electronic environment, Plaintiffs may monitor and track all activity associated with this proprietary information. *Id.*

Plaintiffs' Discovery of Unauthorized Software

On Wednesday, June 1, 2016, Mr. Chen announced that he was resigning his position with Monsanto for the stated reason that he was going to return to Taiwan in order to care for his

ailing father and manage the family business. *Id.* Subsequently, Mr. Chen has admitted that in fact he has received and is considering an offer to serve as Director of Resource Management and Bioinformatics for a seed company in the People's Republic of China. *Id.* On June 1, 2016, the day he announced his resignation, Mr. Chen turned in his computers to Plaintiffs, inconsistent with Company practice. *Id.* Although his job was highly computer-dependent and his last day of work was anticipated to be June 14, 2016, Mr. Chen chose to relinquish his computers at the end of the work day on June 1, 2016. *Id.*

Because of the nature of Mr. Chen's position with the Company, a review of the computers was performed pursuant to company policies. *Id.* At this point, it was discovered that the computers were loaded with highly sophisticated and unauthorized software that could be used to perform reconnaissance, exfiltrate data, and conceal activity on the device. *Id.*

This unauthorized software allows for covert activity within the Company's environment and cloaks the identity of the user through virtual private networks. Declaration of Brent McCarty. It also allows for reconnaissance of the Company's network, using tool sets to understand information such as the Company's IP address configurations, how the Company's electronic architecture is configured, and where external and internal networks intersect. *Id.* The unauthorized software also allows the user to seek vulnerabilities in the Company's environment, including allowing access to areas or files where a user is not allowed, and it also allows for collection of such information. *Id.*

Because of the existence of these unauthorized software programs, the IT department alerted the Director of Business Conduct, who then scheduled an interview with Mr. Chen to inquire about the presence of the software on the machines. Declarations of Scott B. Baucum and Brent A. McCarty. On Thursday, June 9, 2016, Mr. Chen was interviewed regarding this

unauthorized software. In his interview, Mr. Chen denied knowing the concealment software was present on his computers. *Id.*

In addition, Mr. Chen produced at his interviews four different data drives that he stated he had connected to his computers issued to him by Plaintiffs. Mr. Chen stated that he brought these drives to the interview because he "had nothing to hide." *Id.*

However, Mr. Chen was then asked to provide the devices for forensic review, and Mr. Chen refused and referred Plaintiffs to his wife, who also refused permission to relinquish these data drives to Plaintiffs. *Id.*

Plaintiffs' Discovery of Trade Secret Theft

After the interview on June 9, 2016, Plaintiffs continued to monitor activity surrounding Mr. Chen's credentials because of the unauthorized software on the company computers and Mr. Chen's suspicious behavior. *Id.* The credentials themselves that had been assigned to Mr. Chen remained active at this point, but should not have been accessible for the purpose of downloading because the only two computers authorized to perform such downloads from the Company's environment had been relinquished by Mr. Chen on June 1, 2016. *Id.*

In the course of this continued monitoring, it was documented that at 3:47 a.m. on Friday, June 10, 2016, fifty-two files were removed from Plaintiffs' secure environment through the unique account access credentials assigned to Mr. Chen. *Id.* As stated, because Mr. Chen had relinquished the two company computers, no download of data should have been possible using his unique credentials. *Id.*

This documentation was generated by a cloud activity monitoring tool, which interfaces with a cloud source that monitors activity from source to destination. Declaration of Brent

McCarty. Again, this monitoring is part of the Company's substantial efforts to protect its confidential and proprietary information.

A forensic review of the file transfer activity made under Mr. Chen's unique credentials was conducted because the cloud activity monitoring tool typically reports the unique IP address of the computer associated with the activity. *Id.* In this instance, this critical information was not available for any of the fifty-two files transferred at 3:47 a.m. on June 10, 2016. *Id.*

Plaintiffs have carefully reviewed the listing of these files and their content. Plaintiffs have confirmed that the files taken at 3:47 a.m. on Friday, June 10, 2016, contained proprietary material important to Plaintiffs' current and future business. *Id.*

The knowledge or access of these files outside of Plaintiffs' secure electronic environment, particularly by a business competitor, is of great concern to Plaintiffs and would cause them irreparable harm. *Id.*

Mr. Chen's Inculpatory Statements to Plaintiffs

On Tuesday, June 14, 2016, Mr. Chen was scheduled for a routine exit interview. Declarations of Scott B. Baucum and Brent A. McCarty. Following this routine exit interview, Monsanto Director of Business Conduct interviewed Mr. Chen about the fifty-two files that had been removed from the secure environment through the account access credentials assigned to Mr. Chen. *Id.*

During this interview with the Director of Business Conduct, Mr. Chen's demeanor changed noticeably and he made several inculpatory statements. *Id.* First, without in advance knowing the specifics of the intended basis for questioning, Mr. Chen remarked "did you find files moving." *Id.*

Mr. Chen denied having accessed these files but, critically, he confirmed that no one else had knowledge of the unique account access credentials assigned to him. *Id.* Mr. Chen stated his belief that this had been done by a hacker. *Id.*

In addition, Mr. Chen contradicted his statement from June 1, 2016, regarding the reasons for his resignation, and acknowledged that he was seeking employment in the agriculture sector in China. *Id.* Mr. Chen subsequently sent Monsanto unsolicited information that he has in fact received, and is considering, an offer to serve as Director of Resource Management and Bioinformatics for this company in Wuhan, China. *Id.*

Mr. Chen also offered that he had been in contact with Mo Hailong, a Chinese national who recently pleaded to conspiracy to commit theft of trade secrets in United States v. Hailong, Case No. 4:13-cr-147 in the United States District Court for the Southern District of Iowa. *Id.* Contact between Mr. Chen and Mo Hailong occurred during the time Mo Hailong was known to be acquiring Monsanto proprietary germplasm through unauthorized means. *Id.*

Plaintiffs believe that the conduct for which Mr. Hailong pleaded guilty could not have been achieved absent access to inside information. *Id.* Mr. Chen also made statements as to the degree of contact with Mo Hailong that Plaintiffs know to be untrue. *Id.*

Mr. Chen also admitted that in travel to the People's Republic of China on previous occasions, Mr. Chen had learned and was familiar with VPN practices used to cloak his online identity used to circumvent internet access controls by the Chinese government. *Id.* These admitted practices demonstrate the proficiency needed to accomplish the theft of trade secrets as occurred on June 10, 2016. *Id.* Finally, when presented with a listing of the fifty-two files that were transferred under his unique credentials, Mr. Chen acknowledged that all files contained trade secret information. *Id.*

ARGUMENT

I. LEGAL STANDARD

In deciding whether to grant a motion for a temporary restraining order, courts weigh "the movant's probability of success on the merits, the threat of irreparable harm to the movant absent the injunction, the balance between this harm and the injury that the injunction's issuance would inflict on other interested parties, and the public interest." *Pottgen v. Mo. State High Sch. Activities Ass'n*, 40 F.3d 926, 928 (8th Cir.1994). As explained below, all of these factors weigh in favor of the Court granting Plaintiffs' Motion for a Temporary Restraining Order. The DTSA allows the Court wide discretion in granting an injunction "to prevent any actual or threatened misappropriation" of trade secrets "on such terms as the [C]ourt deems reasonable…."

A. There is a Substantial Likelihood Plaintiffs Will Succeed on the Merits.

In Counts I and II of the Complaint, Plaintiffs allege that Defendant misappropriated trade secrets in violation of the Defend Trade Secrets Act of 2016 (18 U.S.C. § 1836(b)(1)), referred to herein as the "DTSA"), and the Missouri Uniform Trade Secrets Act ("MUTSA") (RSMo §§ 417.450 to 417.467), respectively. Plaintiffs' substantial likelihood for success on each of these claims is discussed and demonstrated below.

1. Claim under the Defend Trade Secrets Act

On May 11, 2016, President Obama signed the DTSA, which applies to any act of misappropriation that occurs on or after that date. The DTSA amended the Economic Espionage Act ("EEA"), 18 U.S.C. § 1831, et seq., which was enacted in 1996, and provides as follows:

> An owner of a trade secret that is misappropriated may bring a civil action [in federal court] under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce. *Id.*

The DTSA retained the definition of "trade secrets" under the original EEA, which generally follows the Uniform Trade Secrets Act. Under this definition, the term "trade secrets" covers "all forms and types of" information, including, methods, techniques, processes, procedures, programs, or codes, regardless of how the informtation is stored, where: "the owner thereof has taken reasonable measures to keep such information secret; and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; . . . ." 18 U.S.C. § 1839(3).

The DTSA divides the term misappropriation into two categories: (1) improper acquisition and (2) improper use or disclosure. The DTSA defines improper acquisition as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means." *Id*. Improper use or disclosure is defined as:

> (B) disclosure or use of a trade secret of another without express or implied consent by a person who –
>
> (i) used improper means to acquire knowledge of the trade secret; [or]
>
> (ii) at the time of disclosure or use, knew or had reason to know that his/her knowledge of the trade secret was –
>
> (I) derived from or through a person who had used improper means to acquire the trade secret;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (iii) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; . . . .

Id. The DTSA defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means . . . ." *Id*.

While employed by Plaintiffs, Defendant misappropriated Plaintiffs' trade secrets related to Plaintiffs' products that are used in, or intended for use in, interstate or foreign commerce. Plaintiffs consider the items misappropriated by Defendant to be trade secrets, and Defendant has admitted the information contained trade secrets. Moreover, Plaintiffs took reasonable steps as part of their ongoing standard operating procedures to maintain the confidential nature of this information and Defendant only acquired the information through improper means, including his unauthorized access to Plaintiffs' secure environment where the information was stored. As a result of Defendant's misappropriation, including his unauthorized use and removal of the confidential, proprietary and trade secret information described above, there is a substantial likelihood Plaintiff will prevail in demonstrating that Defendant violated the DTSA.

2. Claim under the MUTSA

There is also a substantial likelihood Plaintiffs will prevail on their claim that Defendant violated the Missouri Uniform Trade Secrets Act ("MUTSA") (RSMo §§ 417.450 to 417.467). To assert a claim under the MUTSA, a claimant must meet three elements: "(1) a trade secret exists, (2) the defendant misappropriated the trade secret, and (3) the plaintiff is entitled to either damages or injunctive relief." *Cent. Trust & Inv. Co. v. Signalpoint Asset Mgmt.*, LLC, 422 S.W.3d 312, 320 (Mo. 2014) (citing RSMo § 417.453; § 417.455 (claims for injunctive relief); and § 417.457 (claims for damages)). As discussed below, Plaintiffs satisfy each element for asserting a claim under the MUTSA.

a. A trade secret exists.

Missouri courts examine the following factors in determining whether allegedly misappropriated information constitutes a trade secret:

> (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of

> measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Healthcare Servs. of the Ozarks, Inc. v. Copeland, 198 S.W.3d 604, 610 (Mo. 2006) (quoting *Continental Research Corp. v. Scholz*, 595 S.W.2d 396, 400–01 (Mo.App.1980).

The trade secret information misappropriated by Defendant: (1) is not known outside of Plaintiffs' business; (2) it is known by very few employees and/or others involved in Plaintiffs' business; (3) Plaintiffs took appropriate measures to protect the confidentiality of the information by storing the information at restricted locations; (4) the information is highly valuable to Plaintiffs and would be highly valuable to Plaintiffs' competitors; (5) Plaintiffs expended considerable time, effort and money developing the information; and (6) it would be very difficult for others to legally acquire and/or duplicate the information. Accordingly, the information misappropriated by Defendant constitutes a trade secret under Missouri law.

b. Defendant misappropriated Plaintiffs' trade secrets.

Under Missouri law, the misappropriation of a trade secret occurs when (1) "a person acquires the trade secret while knowing or having reason to know that he or she is doing so by improper means," (2) "a person who has acquired or derived knowledge of the trade secret discloses it without the owner's consent," or (3) "when a person who has acquired or derived knowledge of the trade secret uses it without the owner's consent." *Cent. Trust & Inv. Co. v. Signalpoint Asset Mgmt., LLC*, 422 S.W.3d 312, 322 (Mo. 2014) (citing § 417.453(2), MUTSA); *see also, Secure Energy, Inc. v. Coal Synthetics, LLC*, 708 F. Supp. 2d 923 (E.D. Mo. 2010) (applying Missouri law).

Here, Defendant knew he was acquiring the Trade Secrets by improper means. This is evidenced by his efforts to covertly obtain the documents using highly sophisticated means

aimed at avoiding detection. When confronted about the theft of the Trade Secrets, Defendant acted surprised Plaintiffs had detected the theft. Moreover, Defendant acquired the Trade Secrets and will no doubt attempt to use them without Plaintiffs' consent.

c. Plaintiffs are entitled to damages and injunctive relief.

The MUTSA provides for injunctive relief and actual damages caused by the misappropriation of trade secrets and for any unjust enrichment caused by the misappropriation. RSMo §§ 417.555, 417.457. The MUTSA also allows for punitive damages where the misappropriation "is outrageous because of the misappropriator's evil motive or reckless indifference to the rights of others." *Id*. at § 417.457.

Because Plaintiffs can demonstrate Defendant has misappropriated its trade secrets, they are entitled to damages and injunctive relief under the MUTSA. Thus, Plaintiffs meet the elements for asserting a valid claim under the MUTSA and have demonstrated a substantial likelihood of prevailing on their claim.

B. A Temporary Restraining Order is Necessary to Prevent Irreparable Harm.

Plaintiffs will suffer irreparable harm if Defendant is not prevented from using and/or disclosing Plaintiffs' trade secrets. The proprietary trade secret information contains sensitive information associated with strategy, building model concepts, and sensitive products of The Climate Company. The information taken explains areas of research for Plaintiffs, the manner in which research is conducted, and research results. Use of the trade secrets in general will deprive Plaintiffs of the value associated with these trade secrets. Here, Defendant has freely admitted that he has received and is considering acceptance of employment with an agricultural company in the People's Republic of China. Dissemination of Plaintiffs' trade secrets in this fashion would cause Plaintiffs irreparable harm.

C. The Balance of the Harms Weighs Heavily in Plaintiffs' Favor.

Defendant cannot credibly claim he will be unfairly harmed by the Court issuing a temporary restraining order. A temporary restraining order puts Defendant in no worse position than had he not acted unlawfully. Defendant has no right to use or disclose Plaintiffs' trade secrets, and he will continue to do so if not stopped by this Court. Moreover, any arguable temporary harm caused to Defendant is outweighed by the potential harm to Plaintiffs should Defendant continue to be allowed to use or disclose their trade secrets, and to otherwise benefit from his unlawful actions. A temporary restraining order will preserve the status quo for a time period during which Defendant could not lawfully have used Plaintiffs' trade secrets, and thus the balance of harms weighs heavily in Plaintiff's favor.

D. Issuing the Temporary Restraining Order Furthers the Public's Interest in Preventing the Misappropriation of Trade Secrets from U.S. Companies.

When President Obama signed the DTSA in May of 2016, which passed in Congress with bipartisan support, he remarked:

> As many of you know, one of the biggest advantages that we've got in this global economy is that we innovate, we come up with new services, new goods, new products, new technologies. Unfortunately, all too often, some of our competitors, instead of competing with us fairly, are trying to steal these trade secrets from American companies. And that means a loss of American jobs, a loss of American markets, a loss of American leadership.

Remarks by the President at Signing of S. 1890 - Defend Trade Secrets Act of 2016, May 11, 2016, available at https://www.whitehouse.gov/the-press-office/2016/05/11/remarks-president-signing-s-1890-defend-trade-secrets-act-2016. As stated by President Obama, the American people, who comprise the public, have an interest in protecting trade secrets developed by American companies from foreigners who seek to steal them.

A temporary restraining order here serves the public interest.

CONCLUSION

Based on the foregoing, Plaintiffs respectfully request the Court enter a temporary restraining order and injunction prohibiting Defendant from further disclosing, transmitting, and/or using Plaintiffs' confidential trade secrets and requiring the return of Plaintiffs' confidential trade secrets, as well as compelling Defendant to identify all cloud data storage accounts along with the user names and passwords for those accounts to allow Plaintiffs to recover its confidential business information and trade secrets misappropriated by Defendant and to conduct analytics on those accounts to determine whether additional transfers occurred.

Respectfully submitted,

HUSCH BLACKWELL LLP

/s/ Matthew T. Schelp
Matthew T. Schelp
Matthew P. Diehr
Mark C. Milton
190 Carondelet Plaza, Suite 600
St. Louis, MO 63105
T: 314.480.1500 / F: 314.480.1505
matthew.schelp@huschblackwell.com
matthew.diehr@huschblackwell.com
mark.milton@huschblackwell.com